cisco
The bridge to possible

Cyber Threat Trends Report:

From Trojan Takeovers to Ransomware Roulette

The bridge to possible

Cyber Threat Trends Report: From Trojan Takeovers to Ransomware Roulette

Contents

The bridge to possible

The threat landscape is always changing. Billions of ever-expanding connections are made every day by organizations across the internet. There are more things to protect than ever before. Work patterns are constantly shifting, which means organizations are more vulnerable against increasingly sophisticated attacks.

Introduction: How DNS Helps Us Discover the Most Dangerous Threats

The domain name system (DNS) was created to connect, not to protect. It was meant to connect users to websites or applications quickly and correctly, and it forms the foundation of internet. People use DNS billions of times a day without knowing it – every time a user connects to a website, opens an app on their phone, or updates software, their device queries DNS servers to find the IP address associated with the domain.

Cisco has a unique vantage point when it comes to cybersecurity. We know that you can't protect what you can't see. Because we resolve an average of 715 billion daily DNS requests, we see more threats, more malware, and more attacks than any other security vendor in the world.

We also power all security services with the threat intelligence of Cisco Talos. Talos is the largest non-governmental threat research organization in the world, made up of an elite group of security experts. These massive data sets and expert security researchers power our threat research and provide unmatched threat intelligence to stop attacks earlier. It's this foundation that lets us see and understand threats sooner and block them faster.

Many of today's sophisticated attacks rely on DNS activity. This report looks at the top threats that exploited DNS for cyberattacks, as well as how DNS-layer security provides better accuracy and detection of malicious activity and compromised systems.

The Domain Name System (DNS) allows clients to connect to websites, perform software updates, and use many of the applications organizations rely on.

Methodology

The following analysis is based off DNS activity observed by organizations using Cisco Umbrella.

The data covers the number of domains blocked between August 2023 through March 2024, based of several threat categories defined by Umbrella.

The trend charts indicate whether the DNS activity in a given month is either up or down when compared to the full time frame's monthly average.

Key Findings

The three most seen threat categories were Information Stealers, Trojans, and Ransomware. Each of these categories had average monthly blocks in the hundreds of millions.

- Information Stealer - 246 Million
- Trojan - 175 Million
- Ransomware - 154 Million
- RAT - 46 Million
- APT - 40 Million
- Botnet - 31 Million
- Dropper - 20 Million
- Backdoor - 14 Million

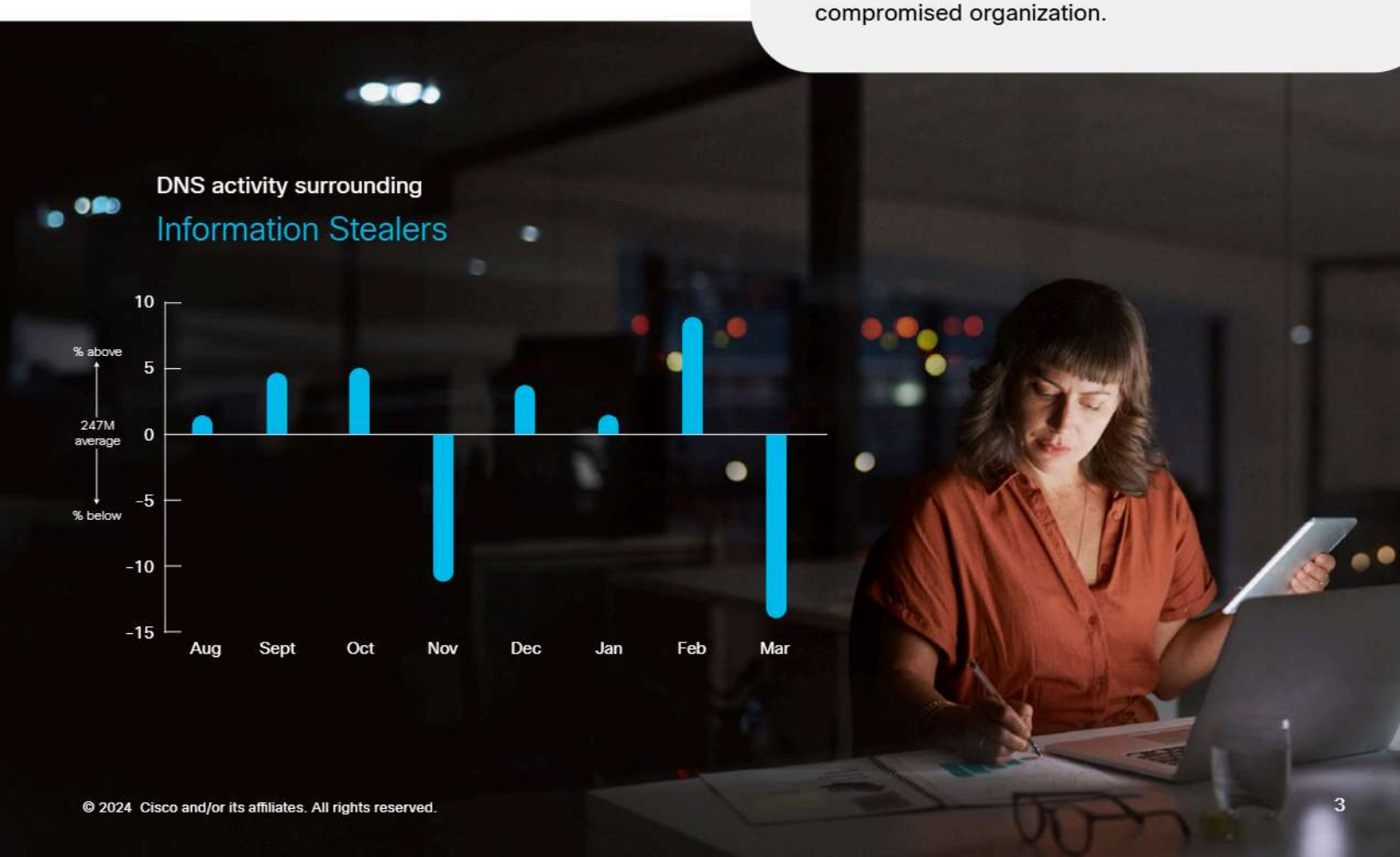
The bridge to possible

Threat #1
Information Stealers

First identified around 2020, Redline has the capability to steal various types of personal information from an infected computer, including stored passwords from browsers, credit card information, cryptocurrency wallets, VPN login credentials, FTP logins, cookies and session data, and more. It's typically delivered via email and malvertising campaigns, either directly or via exploit kits and loader malware; recent research suggests that some cybercriminal groups are targeting the gaming community, leveraging fake Web3 gaming lures to deliver malware capable of stealing sensitive information from macOS and Windows users.

What is an Information Stealer?

Information stealers are malicious programs designed to collect various kinds of personal and financial information from an infected system. They can capture keystrokes, extract files, steal browser data like passwords and cookies, and more. Information stealers generate large amounts of DNS traffic, given that the threat exfiltrates data from a compromised organization.



The bridge to possible

Our analysis – Information Stealers

The Information Stealer activity blocked includes credential stealing and monitoring of audio/video communications. A trend appears with three months of above-average activity, followed by one month of below-average activity. These drops in activity could be tied to attack groups processing large caches of stolen data—collect for three months, then analyze for one. This is something that's been seen before in the threat landscape over time.

Information stealers persist as a significant threat because they can covertly harvest a wealth of sensitive data, which is highly valued on the black market. The continuous creation of new variants can evade detection, and the broad range of tactics for distribution, including phishing and compromised websites, ensures a steady stream of victims. As personal and financial data remain lucrative targets, information stealers are consistently updated and deployed by cybercriminals.

Threat #2

Trojans

Qakbot is a multifunctional and sophisticated Trojan with capabilities that include stealing banking credentials and other personal information, as well as providing a backdoor for attackers to install additional malware on infected systems. Over time, QakBot has evolved with various updates and improvements to its evasion and propagation techniques. It can propagate itself across networks by exploiting vulnerabilities and using brute force attacks on account credentials, allowing it to spread rapidly within corporate networks.

What is a Trojan?

Trojans are a type of malware that mislead users of their true intent. They are often disguised as legitimate software; another common installation tactic is when a user gets a malicious link, like an email attachment disguised as an invoice, that once clicked on can silently install a Trojan. Once activated, they can enable cybercriminals to spy on you, steal your sensitive data, and gain backdoor access to your system.

The bridge to possible

DNS activity surrounding

Trojans

Our analysis – Trojans

Trojan activity was highest in August and September 2023, then declined over the remaining time frame of this research. Despite the declines, Trojan activity is the second-highest across the threat categories. In the past, Trojan activity drops have been seen alongside spikes in ransomware.

Trojans continue to be a common threat due to their deceptive nature and ability to hide in the background while performing malicious activities. They are an effective means for attackers to gain unauthorized access to systems, deliver additional malware, and create backdoors. The ease with which Trojans can be spread through social engineering and software vulnerabilities contributes to their ongoing prevalence in our threat reports.

The bridge to possible

Threat #3

Ransomware

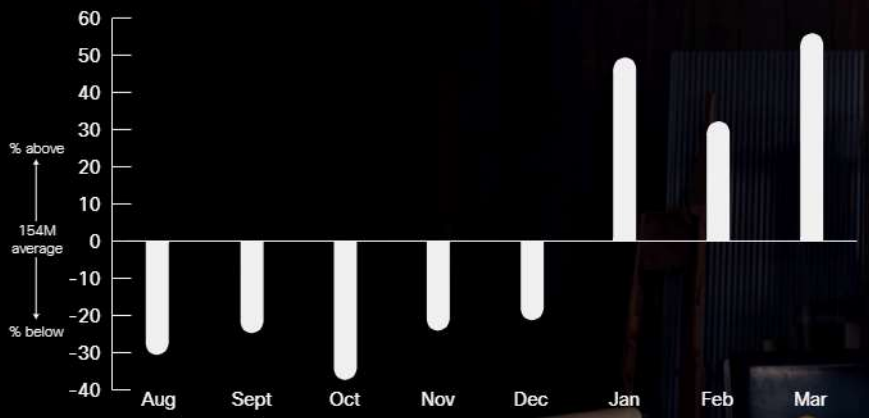
Lockbit is one of the more active ransomware variants today; its ransomware operations accounted for over 25 percent of the total number of posts made to data leak sites. In February 2024, multi-agency international law enforcement task force managed to disrupt LockBit operations. However the group managed to quickly resume operations, utilizing new servers and encryptors.

What is Ransomware?

Ransomware is a type of malware that encrypts the files on a victim's computer or network, making them inaccessible, and demands a ransom payment to decrypt them. Victims are often threatened with permanent loss of data or exposure of stolen data if the ransom isn't paid.

DNS activity surrounding

Ransomware



Our analysis - Ransomware

Ransomware activity jumped in January and stayed high for the rest of the observed time frame. The trends seen in ransomware closely shadow the trends seen in the dropper category, suggesting a correlation between the two. It's likely that the droppers we're seeing are being used to seed ransomware payloads. Ransomware remains a prevalent threat as it directly monetizes attacks by holding data or systems hostage for ransom. It's high profitability, coupled with the increasing availability of ransomware-as-a-service platforms, allows even less skilled attackers to launch campaigns. Organizations' often inadequate backup and recovery processes, and the willingness of many to pay the ransom, perpetuate the cycle of attacks.

The bridge to possible

Threat #4

RAT (Remote Access Trojans)

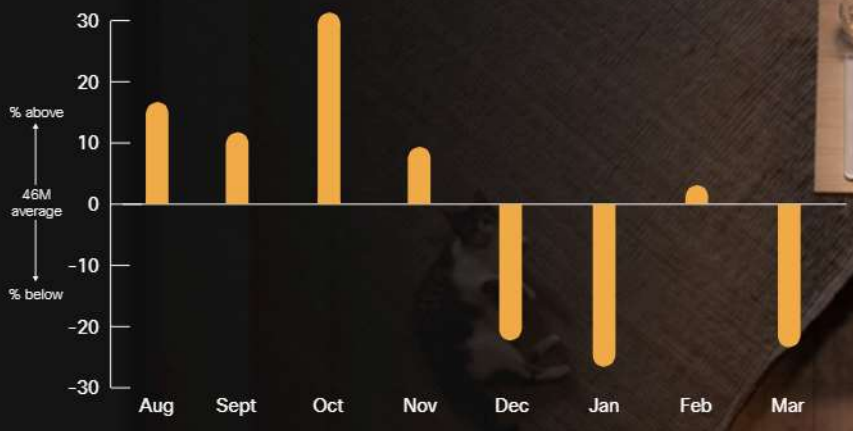
As early as 2009, a RAT known as Gh0st RAT was used in targeted attacks. It's known for its stealthiness and for being difficult to detect. It allows attackers to take full control over the infected device and has been used in espionage campaigns. Cisco Talos Threat Intelligence noted that this threat has evolved, citing a malicious campaign that likely started as early as August 2023, delivering a new RAT dubbed "SugarGh0st", with evidence suggesting the threat actor is targeting the Uzbekistan Ministry of Foreign Affairs and users in South Korea. SugarGh0st RAT is a new customized variant of Gh0st RAT, an infamous trojan that's been active for more than a decade, with customized commands to facilitate the remote administration tasks as directed by the C2 and modified communication protocol based on the similarity of the command structure and the strings used in the code.

What is a Remote Access Trojan?

RATs are a type of malware that provide a backdoor for administrative control over the targeted computer. RATs enable intruders to do almost anything on the targeted computer, such as monitoring user behavior, accessing confidential information, activating the system's webcam, and distributing more malware.

DNS activity surrounding

Remote Access Trojans (RAT)



The bridge to possible

Our analysis - Remote Access Trojans (RAT)

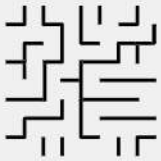
Like Trojan activity, RAT activity has trended down over the time frame. A spike in activity seen in October coincides with a similar spike in Backdoor activity. It's possible that this spike could be caused by the release of an updated version of Cobalt Strike; version 4.9 was released in late September.

RATs continue to be a favored tool for cybercriminals and espionage due to their ability to provide deep access to compromised systems. They enable stealthy surveillance, data exfiltration, and full control over victim machines, often remaining undetected for extended periods. The difficulty in detecting RATs and their multifunctional use in targeted attacks ensures their persistence in threat landscapes.

Threat #5

APT (Advanced Persistent Threats)

Cisco Talos Threat Intelligence has identified a new threat authored and operated by the Turla APT group, a Russian cyber espionage threat groupm, called "TinyTurla-NG" (TTNG) (similar to Turla's previously disclosed implant, TinyTurla, in coding style and functionality implementation). Talos assessed that that TinyTurla-NG, just like TinyTurla, is a small "last chance" backdoor that is left behind to be used when all other unauthorized access/backdoor mechanisms have failed or been detected on the infected systems.



What is an Advanced Persistent Threat?

APTs are complex, sophisticated threats that target specific entities (like organizations or nations) with the intent to steal information or disrupt operations. These threats are persistent, often remaining undetected in a network for a long time, and are carried out by well-funded cybercriminals or state-sponsored groups.

cisco
The bridge to possible

DNS activity surrounding
Advanced Persistent Threats (APT)

Our analysis - Advanced Persistent Threats (APT)

This category, while averaging 40 million blocks a month, had one of the lowest rates of change—or most stable amount activity—from one month to the next. This classification covers highly skilled threat actors with resources, time, and dedication to carry out sophisticated attacks.

APTs remain prevalent because of their sophisticated, targeted, and stealthy nature, often backed by nation-states or well-funded entities. Their long-term focus on espionage and intellectual property theft, combined with their ability to remain undetected within networks for months or years, makes them a continually evolving and persistent threat in cybersecurity.

The bridge to possible

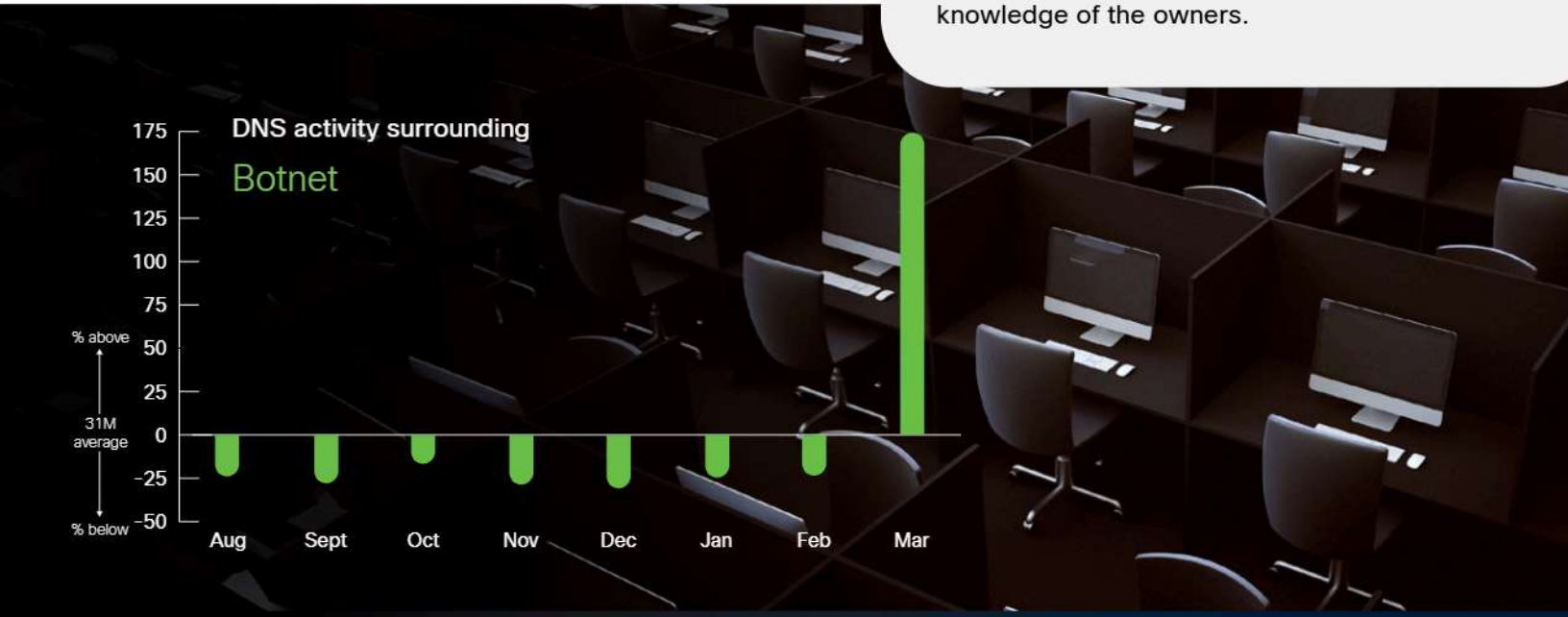
Threat #6

Botnet

The Mirai botnet is a well-known example. In 2016, it was used to launch a massive DDoS attack that took down large parts of the internet, including services like Twitter, Netflix, and Reddit. The botnet was primarily composed of IoT devices like cameras and DVRs that were infected by exploiting default usernames and passwords. Another Linux-based botnet, TheMoon, has been growing in the first part of 2024, reaching 40,000 endpoints in 88 countries.

What is Botnet?

A botnet is a network of infected computers, known as bots, which are controlled by a threat actor (often called a "botmaster"). These compromised computers can be controlled remotely to perform malicious activities such as launching Distributed Denial-of-Service (DDoS) attacks, sending spam emails, stealing data, or spreading malware without the knowledge of the owners.



Our analysis - Botnet

Botnet activity remained fairly stable over the observed time frame, until a sudden spike in activity in March, which was 174% above the average for the time frame.

Overall, Botnets remain a prevalent cyber threat due to their ability to rapidly propagate across a vast number of devices, including insecure IoT devices, and their versatility in executing a range of malicious activities such as DDoS attacks and data theft. They are challenging to detect and dismantle because of their decentralized command-and-control structures and stealthy operation.

The bridge to possible

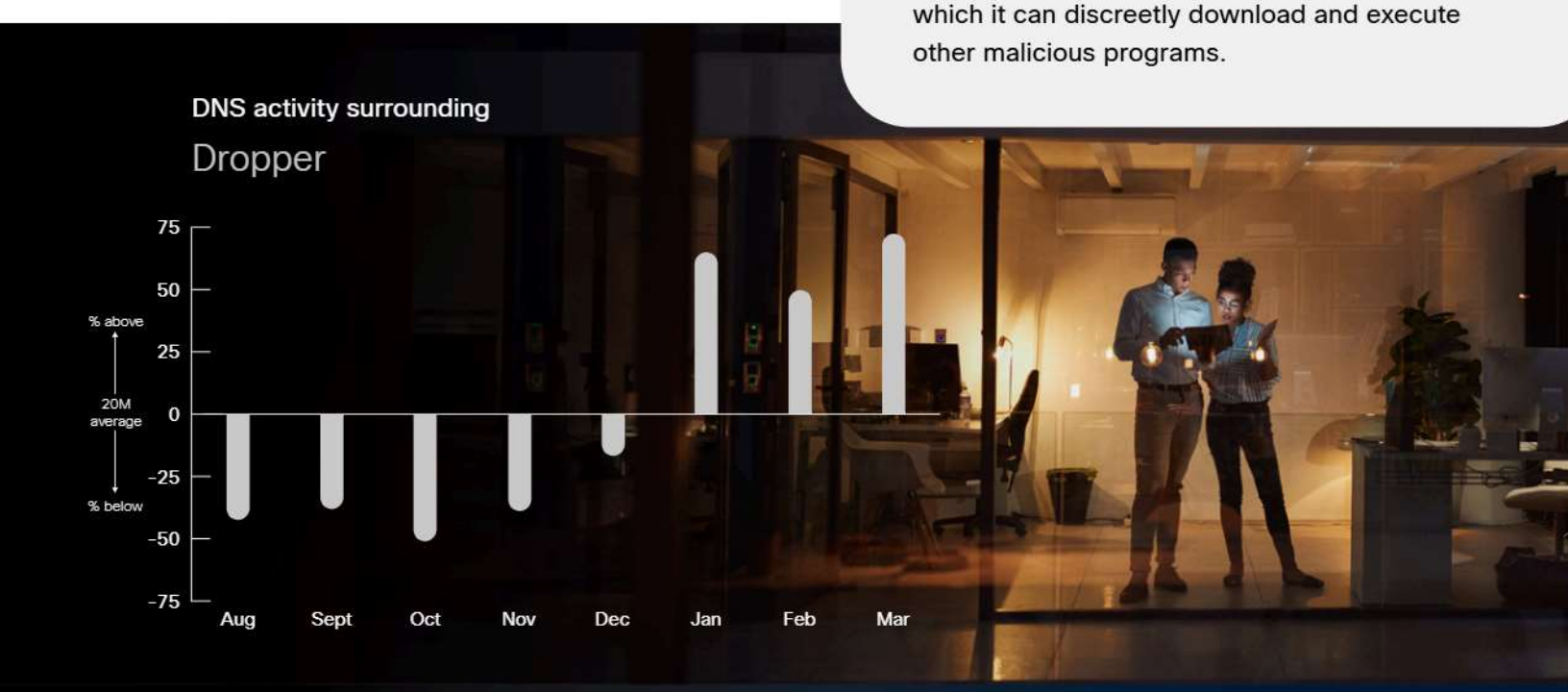
Threat #7

Dropper

In 2019, a dropper known as “xHelper” emerged, targeting Android devices. It was notorious for its persistence, being able to reinstall itself after attempts to remove it manually or even after factory resets. xHelper would download and install other malicious applications that could carry out various nefarious activities.

What is a Dropper?

A dropper is a type of malware designed to install other malwares onto a target system. The dropper itself does not typically cause harm to the system; instead, its purpose is to evade detection and establish a foothold, from which it can discreetly download and execute other malicious programs.



Our analysis - Dropper

Like the Ransomware category, the dropper category saw a jump in activity in January that continued through the end of the time frame.

Droppers are still commonly reported as they play a crucial role in multi-stage malware attacks by facilitating the discreet delivery of payloads. Their ability to bypass initial security measures and subsequently install more destructive malware makes them a persistent tool in the cybercriminal arsenal. As droppers evolve to evade detection, their use in facilitating complex malware infections keeps them relevant.

The bridge to possible

Threat #8

Backdoor

Cobalt Strike is a legitimate software tool used primarily for penetration testing and security assessments. However, its powerful capabilities have also been co-opted by cybercriminals for malicious purposes. As a security threat, Cobalt Strike refers to the unauthorized use of the Cobalt Strike toolset by attackers. Cybercriminals use Cobalt Strike's "beacon" payloads for command and control (C2) of compromised systems within a target network. Malleable C2 profiles allow attackers to customize the beacon's network traffic to blend in with normal traffic, making it harder for network defense systems to detect malicious communications. It also provides a suite of tools for post-exploitation activities, including privilege escalation, lateral movement, and reconnaissance, which attackers can use to further their foothold within a network.

What is a Backdoor?

A backdoor is a method by which unauthorized users can bypass normal authentication and gain remote access to a computer or network. It may be an installed software or a built-in feature of the hardware or software.

The bridge to possible

Our analysis - Backdoor

The majority of backdoor activity observed can be attributed to the use of Cobalt Strike. A spike in activity seen in October coincides with a similar spike in RAT activity. It's possible that this spike could be attributed to the release of version 4.9 of Cobalt Strike.

Backdoors remain a significant threat as they provide attackers with ongoing, unauthorized access to compromised systems. Their stealth and persistence enable long-term exploitation for data breaches, surveillance, or further malicious activities. The strategic placement of backdoors within software or systems, often through supply chain compromises, makes them a challenging threat to eliminate and a consistent concern for organizations.

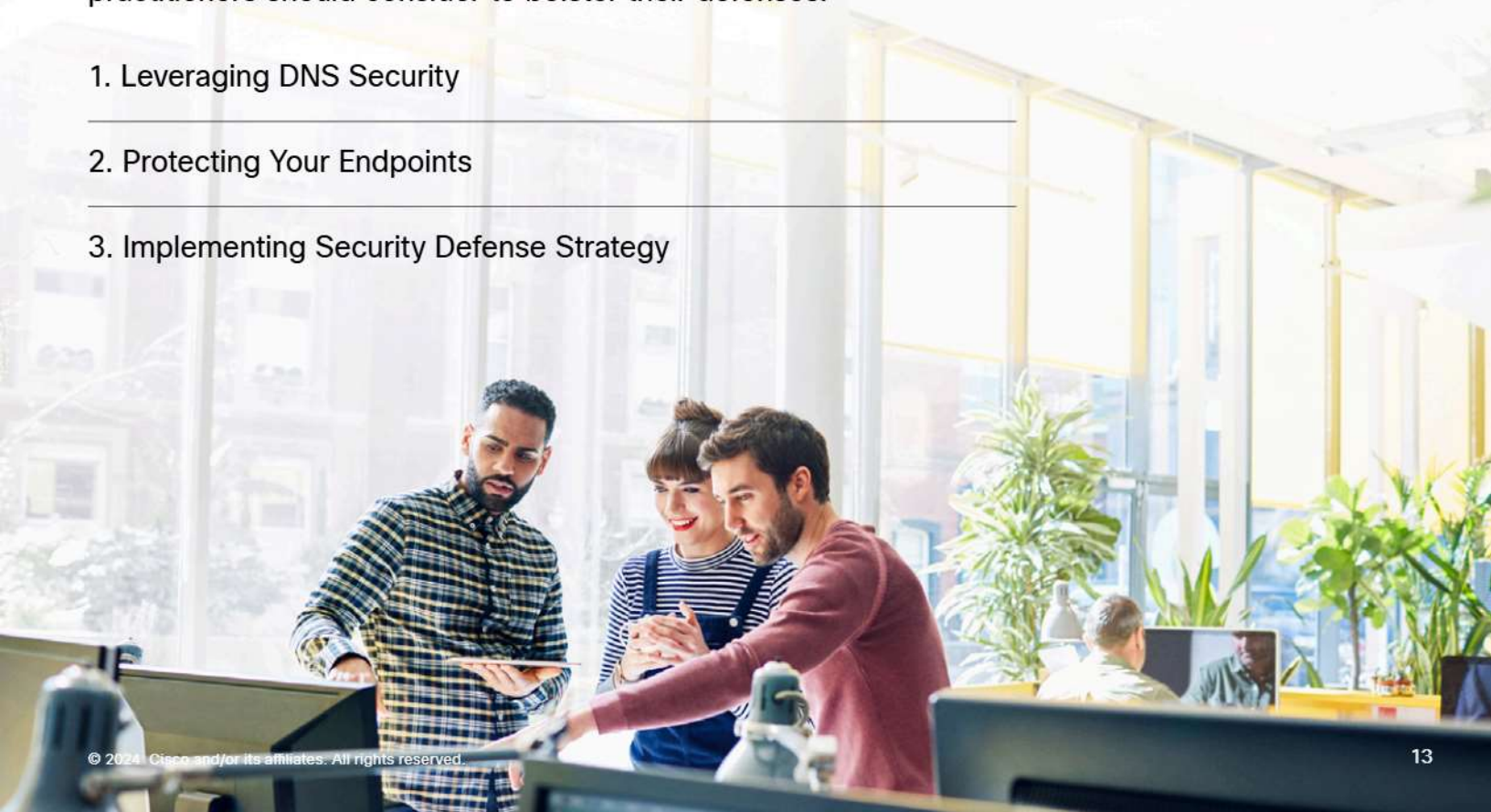
Recommendations

By monitoring and controlling DNS queries, security practitioners can often identify and block malicious traffic before it reaches end-users devices. Here are some recommendations and next steps security practitioners should consider to bolster their defenses:

1. Leveraging DNS Security

2. Protecting Your Endpoints

3. Implementing Security Defense Strategy

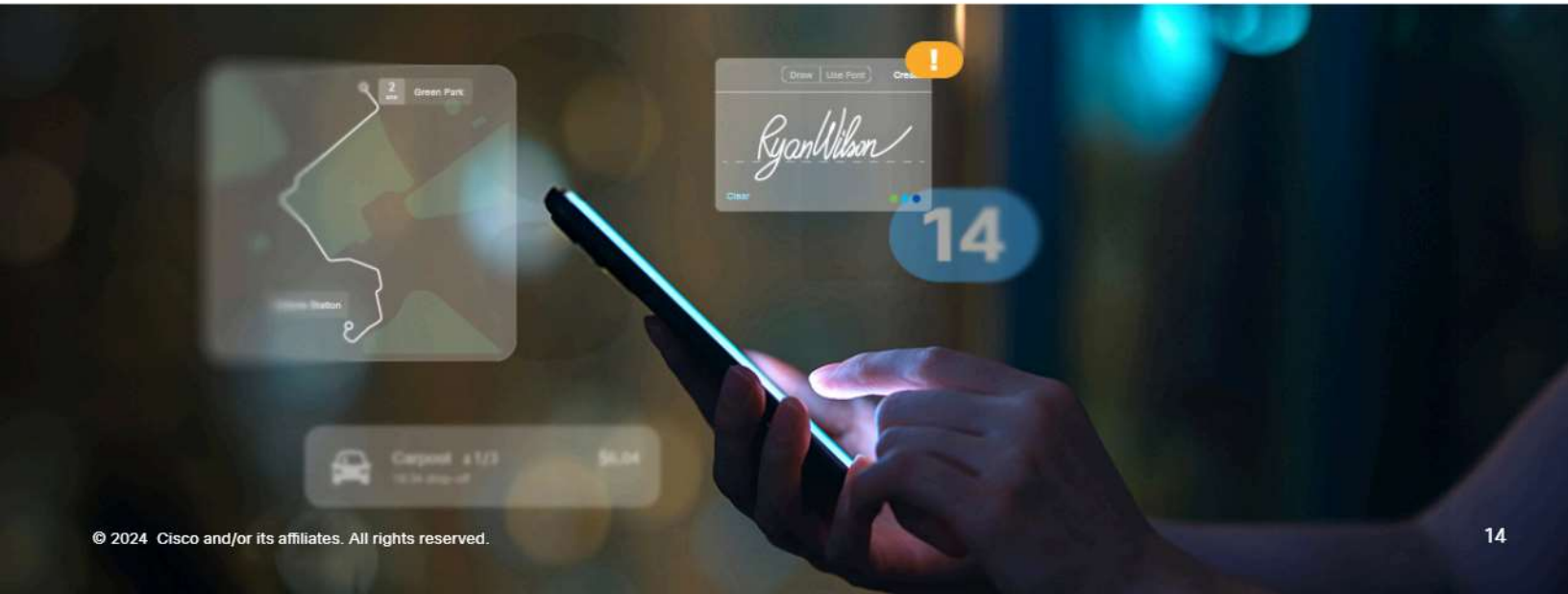


Leveraging DNS Security

- **Implement DNS filtering:** Use DNS filtering services to block access to known malicious domains and IP addresses. This can prevent connections to command-and-control servers, phishing sites, and other malicious online resources.
- **Leverage threat intelligence:** Integrate threat intelligence feeds with your security systems to keep the list of malicious hosts up to date. This proactive approach helps to identify and block new threats as they emerge.
- **Monitor DNS traffic:** Regularly monitor and analyze DNS logs for unusual patterns that may indicate malicious activity, such as a high number of DNS queries, repeated queries for non-existent domains (NXDOMAIN), or frequent queries to a single domain.
- **Secure DNS resolvers:** Ensure that your DNS resolvers are securely configured to prevent DNS hijacking and cache poisoning attacks. Use DNSSEC (DNS Security Extensions) to protect the integrity of DNS data.

Protecting Your Endpoints

- **Segment networks:** Segment your network to limit the spread of malware. If a device is compromised, network segmentation can prevent the malware from moving laterally to other parts of the network.
- **Endpoint protection:** Deploy advanced endpoint protection solutions that can detect and block malware, including zero-day threats, by using behavioral analysis and machine learning techniques.
- **Implement access controls:** Use the principle of least privilege and strong authentication methods to minimize the potential impact of a backdoor or RAT that gains access to a system.



Implementing Security Defense Strategy

- **Patch and update systems:** Keep all systems and software updated with the latest patches to protect against known vulnerabilities that could be exploited by malware such as Trojans, droppers, and backdoors.
- **Educate users:** Train employees on security best practices to help them identify phishing attempts and other social engineering tactics that could lead to malware infections.
- **Regularly backup data:** Conduct regular backups of critical data and ensure that these backups are stored securely and can be restored quickly. This is particularly important to recover from ransomware attacks.
- **Plan incident response:** Develop and regularly test an incident response plan so that your organization is prepared to respond effectively to cybersecurity incidents.
- **Create a multi-layered defense strategy:** Use a layered approach to security, combining DNS-layer security with other security controls such as firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS).

How DNS Security Can Defend Against Top Threats and Increase Security Resilience

According to the Global Cyber Alliance's Value of DNS Security report, DNS security can mitigate one-third of cyber incidents, preventing up to $10 billion in losses. Securing the DNS layer means blocking malicious domains, IP addresses, and cloud applications before a connection is ever established.

Cisco is a global leader in DNS-layer security; we see 550 billion security events every day, 1.5 billion authentication requests per month, 2.8 million new samples of malware per day and discover over 200 vulnerabilities per year. Because we have end-to-end visibility, we can protect against more threats. With over 30,000 customers already choosing Cisco as their trusted partner in DNS security, organizations can be confident that their users will be better protected through their ongoing hybrid work, cloud transformation, and distributed environments.

The bridge to possible

About Security Service Edge (SSE)

Security Service Edge (SSE) architecture focuses on providing secure access to services, applications, and data across a distributed network, including cloud environments, remote locations, and mobile users. By unifying multiple security functions, including DNS security, into a cloud service, SSE effectively protects both users and infrastructure from threats.

About Cisco Umbrella

Cisco Umbrella is part of the Cisco Security Service Edge (SSE) product family, powering secure internet access for all Cisco SSE solutions. Umbrella uses DNS to stop threats over all ports and protocols to stop malware earlier and prevent callbacks to attackers if infected machines connect to your network. Umbrella gives organizations of all sizes the data and visibility they need to block more threats faster with fewer false positives.

As a leader in robust DNS-layer security, Umbrella provides an added layer of protection for users on-premises, while also ensuring roaming users get reliable protection for wherever their work takes them. Deploy and begin stopping threats in as soon as one day.

Schedule a Cisco Umbrella Demo

About Cisco Secure Access

Cisco Secure Access is the newest addition to our Security Service Edge (SSE) product family, and combines converged, cloud-delivered security, zero trust principles, and AI-enhanced visibility to radically improve organizations' ability to provide secure access from anything to anywhere.

Secure Access provides an extended set of security capabilities, including secure web gateway (SWG), cloud access security broker (CASB), zero trust network access (ZTNA), remote browser isolation (RBI), data loss prevention (DLP), cloud malware detection, and more. It effectively secures user access to the Internet, public SaaS apps, and private apps, protecting them against sophisticated, evolving threats.

Schedule a Cisco Secure Access Demo